Systems and Network Analysis Center
Information Assurance Directorate

How to Securely Configure Microsoft® Windows Vista™ BitLocker™

OVERVIEW

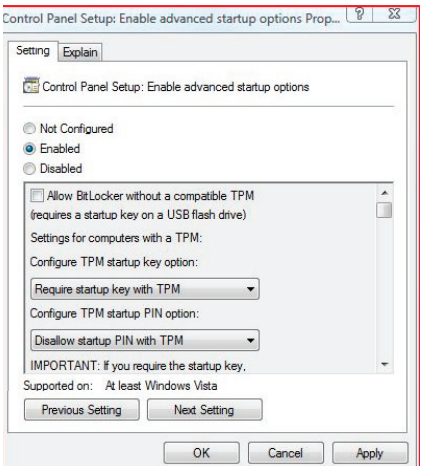
THE CHALLENGE

Personal information or trade secrets can quickly be recovered from laptop hard drives that are not protected by encryption.

A SOLUTION

Microsoft has provided a full volume encryption product, BitLocker, in the Enterprise and Ultimate Editions of Microsoft Windows Vista. BitLocker can be used for full volume encryption of the operating system partition and data partitions. BitLocker can also provide Secure Startup capabilities, so the user is assured that the computer has not been tampered with since the last boot. This guide describes a suggested security configuration for authentication, recovery, and algorithms. It should in no way be construed as an NSA endorsement of the product.

1. BitLocker supports several different methods of authentication, which include the TPM (Trusted Platform Module), a USB key, and a PIN. A Version 1.2 compliant TPM should always be one of the factors for authentication. Although BitLocker can operate without a TPM, it is not recommended. The default for BitLocker is single factor authentication with a TPM. We recommend using the TPM plus a USB key. The Microsoft Management Console (MMC) can be used to change group policy settings, allowing for multifactor authentication.



All group policy settings for BitLocker can be found by the following path:

MMC -> Group Policy Object -> Computer Configuration -> Administrative Templates -> Windows Components -> BitLocker Drive Encryption

2. By using BitLocker with a TPM, Secure Startup will be invoked automatically, which helps to protect from boot code attacks. The amount of protection gained by using Secure Startup can be adjusted under the group policy setting "Configure TPM Platform Validation Profile." We recommend using the default configuration.

3. BitLocker supports both AES-128 and AES-256. Either of these modes can be used with or without a Microsoft proprietary diffuser. We recommend using group policy to configuring BitLocker to use "AES-256 bit with Diffuser". This can be set in the "Configure Encryption Method" group policy setting.

SNAC DoD, 9800 Savage Rd Ft. Meade, MD 20755-6704 410-854-6632 DSN 244-6632 FAX: 410-854-6604 www.nsa.gov/snac

TOP 7 THINGS TO DO When Using BitLocker

1. Use multifactor authentication. Never store a USB token used for authentication with the laptop it is protecting.

2. Use a TPM, Version 1.2 to leverage Secure Startup, which provides a chain of trust during power up.

3. Use AES-256 encryption with a diffuser.

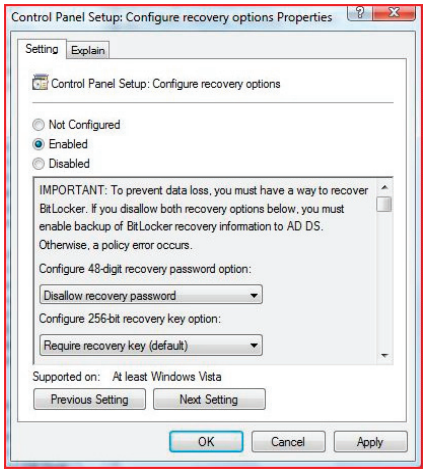
4. Never store the recovery mechanisms with the device they protect.

5. Disable Sleep mode when using BitLocker since a return from Sleep does not require re-authentication.

6. BitLocker should never be disabled once it has been turned on.

7. Set a strong BIOS password so the TPM cannot be reset by unauthorized users.

4. BitLocker supports two recovery methods in the event of a lost token or forgotten PIN. When BitLocker is initialized, a recovery password or a recovery key can be created. A recovery password is a 48-digit password that can be printed. A recovery key is a 256-bit key that is stored on a USB token. We recommend using the recovery key since it is cryptographically stronger than a recovery password. Neither the recovery password nor the recovery key should ever be stored with the encrypted device.



5. The Sleep state should be disabled, as BitLocker authentication is not required when the computer resumes from Sleep. Sleep can be disabled in the Control Panel under Power Options. BitLocker requires authentication when resuming from Hibernation. If the computer is left unattended, then the Hibernate state should be enabled or the machine should be powered-off.

6. Once BitLocker has been turned on, it should never be disabled. When BitLocker is disabled, the encryption key is exposed on the hard drive. If it has to be disabled for any reason, the computer is no longer secure and the volume should be decrypted. BitLocker should then be re-enabled, which will cause a new encryption key to be generated.

7. When using BitLocker with a TPM, a strong BIOS password should always be set to prevent unauthorized users from resetting the TPM. If a TPM is intentionally or accidentally reset, the encrypted data will still be secure but a recovery key or recovery password will be needed to unlock the drive and boot the system.

SNAC DoD, 9800 Savage Rd Ft. Meade, MD 20755-6704 410-854-6632 DSN 244-6632 FAX: 410-854-6604 www.nsa.gov/snac

i036040